

**WPI0040**

**EMERGENCY SYSTEM SECURITY PATCH PROCESS**

# EMERGENCY SYSTEM SECURITY PATCH PROCESS

## 1 BACKGROUND

- 1.1 What is an Emergency System Security Patch
- 1.2 What is a Security Alert
- 1.3 Other Factors
- 1.4 The Big Picture

## 2 SCOPE

## 3 PURPOSE

## 4 OBJECTIVE

## 5 PROCEDURE

- 5.1 Overview of the process
- 5.2 Security Engineering Responsibilities
- 5.3 Configuration Management Responsibilities
- 5.4 Security Engineering Responsibilities
- 5.5 Radar Operations Team (ROT) Responsibilities
- 5.6 Documentation Team (DT) Responsibilities
- 5.7 Flowchart of ESSPP

## 1. BACKGROUND

As the NEXRAD Product Improvement (NPI) project is implemented and open systems are deployed to field sites, the likelihood of a situation arising where an Emergency System Security Patch (ESSP) is required increases.

### 1.1 What is an Emergency System Security Patch?

A software patch is defined by NIST (National Institute of Standards and Technology) as: a piece of software released by a software manufacturer to correct a bug. In the context of this document the definition of a system patch will not only encompass the NIST definition but will also include any modification of system code (such as disabling a service or a feature). What then constitutes an ESSP? Three criteria must be met before an ESSP situation for NEXRAD exists. First an emergency situation impacting security must exist. Who makes this determination? In regards to NEXRAD an emergency situation impacting security is determined when any or all of the tri-agencies issue(s) a security alert.

### 1.2 What is a Security Alert?

The tri-agencies' procedures to address vulnerabilities or threats to information systems (IS) are similar in their process, yet distinct in their terminology and chain of command. Each of the tri-agencies has a process, which receives information regarding a vulnerability or a threat, evaluates this information and disperses this information (alert) to subordinate agencies (NEXRAD). These alerts are rated by their severity and their probability of occurrence. This ESSPP is written to address security alerts issued by any of the tri-agencies with a rating, which requires immediate response.

### 1.3 Other Factors

The issuance of a security alert is not the only factor to determine if an Emergency System Security Patch (ESSP) is required for a NEXRAD system. The second criteria that must be met

is that a security alert must also be relevant to the specific information system (IS) used by NEXRAD. For example, NEXRAD does not have Apple Computers so security alerts issued by DOC, DOD, or DOT for Apple Software are not applicable to NEXRAD. The third criteria to determine if an ESSP situation exists is whether a patch is available. Therefore for an ESSP situation to exist all of the below must be true:

1. A security alert with an emergency rating must be issued by one of the tri-agencies
2. A NEXRAD system must be vulnerable to the security alert
3. A patch, if applicable, must be available.

#### **1.4 The Big Picture**

The Emergency System Security Patch Process (ESSPP) is part of the more comprehensive Security Alert Process (SAP). The SAP addresses the NEXRAD process for tracking and responding to all security alerts issued by the tri-agencies. Some of these security alerts are informative in nature and require no response, but still need to be documented. Most security alerts require a response of some kind. If the security alert is not applicable to a NEXRAD system, then a short “We are not impacted” statement may suffice. If the security alert is applicable to a NEXRAD system but the issued alert does not require immediate action then the issuing agency will be informed that the patch will be applied to the next build cycle. The ESSPP is a modular process of the broader SAP. After the ESSPP has been finalized, Security Engineering will complete the SAP and submit it to the Security Working Group for review and approval.

### **2. SCOPE**

This Emergency System Security Patch Process is a process internal to the ROC, and specific to NEXRAD. This ESSPP only applies to commercial off the shelf (COTS) products; it does not apply to the RPG, OPUP, or ORDA application software. A separate process will cover the application software security process

### **3.OBJECTIVE**

The immediate objective is to establish a process that will enable NEXRAD to address a situation where an emergency system patch is required. Once this process is established the intent is to refine and enhance the process. The final objective is to expedite the process as much as possible. The amount of time required to complete the process for individual patch requirements is to be in accordance with guidelines from DOD, DOC, and DOT.

### **4. PURPOSE**

The purpose of the ESSPP is to:

1. Establish a process that meets the guidelines from DOD, DOC, and DOT.
2. Outline the roles and responsibilities for ROC sections involved with the process.

### **5. PROCESS**

#### **5.1Overview:**

The process portion of this document is organized by ROC sections, with bullets indicating the steps within each section. Bullets were used instead of numbers, because many of these steps will be concurrent.

#### **5.2 Security Engineering:**

- Notify all ROC personnel involved with the ESSPP.

- Coordinate with Configuration Management and Software Engineering to convey any information needed regarding the alert.
- Notify the Hotline of pending system security patch with basic information about the security issue.
- Security Engineering will lead a scope of effort analysis to evaluate cost, extent of resources required and to inform management of the impact.
- Report solution, status and possibly a time compliance estimate back to the issuing agency.
- Coordinate with the Documentation Team as needed.
- Coordinate with the Radar Operations Team (ROT) as needed.
- Provide status updates to all relevant ROC sections on a day-to-day basis.
- Report Security Patch compliance back to issuing agency.
- Update this process to reflect new policies and procedures.

### **5.3 Configuration Management:**

- Work with Software Engineering to submit an emergency CCR.
- Create a Razor Issue.
- Forward baselined software build to Software Engineering.
- Interface with Documentation Team regarding Mod Notes if necessary.
- Receive finished Mod note from Documentation.
- Receive finished Patch release (checked into Razor) from Software Engineering.
- Build Patch Release CD.
- Forward Patch Release to ROT for testing.
- Once ROT has tested the Patch release and checked the Patch release back into Razor, approval of release distribution must be obtained for the patch to be distributed to the field.
- Distribute patch kit (including patch CD and Mod note) to WSR-88D field sites and the Hotline.
  1. Reproduce CDs, including MSCF and BDDS (more than 170).
  2. FedEx patch kit to sites.
- Confirmation of Patch from field sites
  1. NWS sites (121 sites) – reports through Engineering Management Reporting System (EMRS).
  2. DOD and FAA sites - return signed sheet of Mod notes to CM.
- CM will ensure that this patch release will be baselined for the next Build cycle.

### **5.4 Software Engineering**

First step is for Software Engineering and CM to come up with a Generic Security Patch Script With Procedures (GSPSWP) waiting “on the shelf”. We will try to have something ready in the Build 5.0 time frame. We can further refine the process after build 5.0.

Software Engineering Security Responsibilities:

- Software Engineering will download the patch from the vendor.
- Software Engineering will perform *limited* (depending on the time available) unit testing and integration (CPCI level) testing to ensure the patch has not impacted application software.

- Software Engineering will coordinate unit testing details with ROT.
- Software Engineering will work with CM to get an emergency CCR and Issue generated so the patch can be put into Razor.
- Hopefully, the patch will be seamlessly integrated into GSPSWP.
- If the security patch is successfully integrated into GSPSWP, no extra installation documentation will be needed.
- If the security patch is NOT successfully integrated into GSPSWP. New documentation will have to be generated with the help of ROT and coordinated with the documentation group.
- Software Engineering will provide a copy of the draft documents to DT.
- Software Engineering will check software changes into Razor, which CM will use to build Patch release CD to be sent to ROT.

### **5.5 Radar Operation Team (ROT):**

- ROT will coordinate/communicate with Software Engineering to assess extent of the Patch on the system and application software, and to ensure that duplication of test processes does not occur.
- Once Testing receives the CCR and the Patch Release (CD) from CM, ROT staff will evaluate the extent of testing required based on the following:
  1. Does the Software Patch impact the ORPG/OPUP application software? If the Patch does impact the application software, testing will be more extensive. Perform test based on initial SWE analysis.
  2. Do all configurations (FAA, DOD, NWS single, NWS redundant, MLOS) need to be tested? This decision would be based on the scope of the changes.
  3. Do all phases (integration, system, operations, beta, etc) of testing need to be implemented? Some of these phases may be bypassed depending on the impact of the patch to the system and the relevance of the patch to the application software.
- Any Security System Patch must include a 24-hour stability test as part of the required testing.
- ROT will approve release but kit will not be shipped without tri-agency CCR approval.

### **5.6 Documentation Team (DT):**

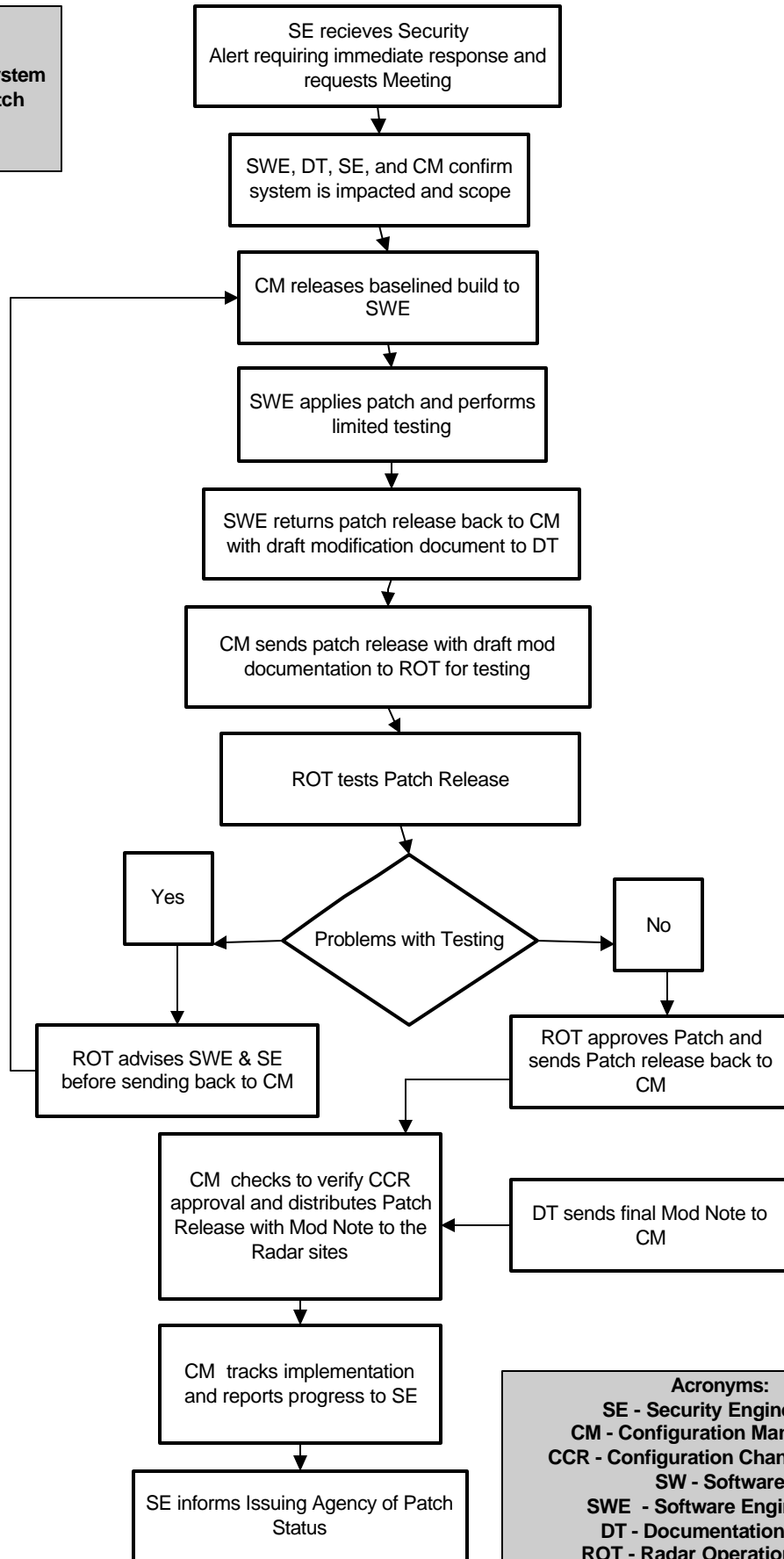
- Confirm with DOD, NWS and FAA that the format (agreed upon by all) can be used for the Emergency patch process mod note.
- Create a template (one each for ORPG, ORDA, OPUP) for the Emergency Patch process Mod note. These templates could be used with a few minor changes for each specific patch?
- Receive mod note from SWE.
- Once the Mod note is cleaned up and signatures acquired, then forward to CM for distribution of the Mod notes.
- Forward to SE for review and archive.
- Perform a quick print (3 day print cycle) if necessary.
- The completed and signed Mod note is sent to CM for distribution.

### **5.7 Flowchart of ESSPP:**

A series of six flowcharts provide a visual representation of the ESSPP. The first flowchart provides an overview of the process and the contiguous steps required for a patch to be applied to the system. The next five flowcharts summarize the internal steps that must

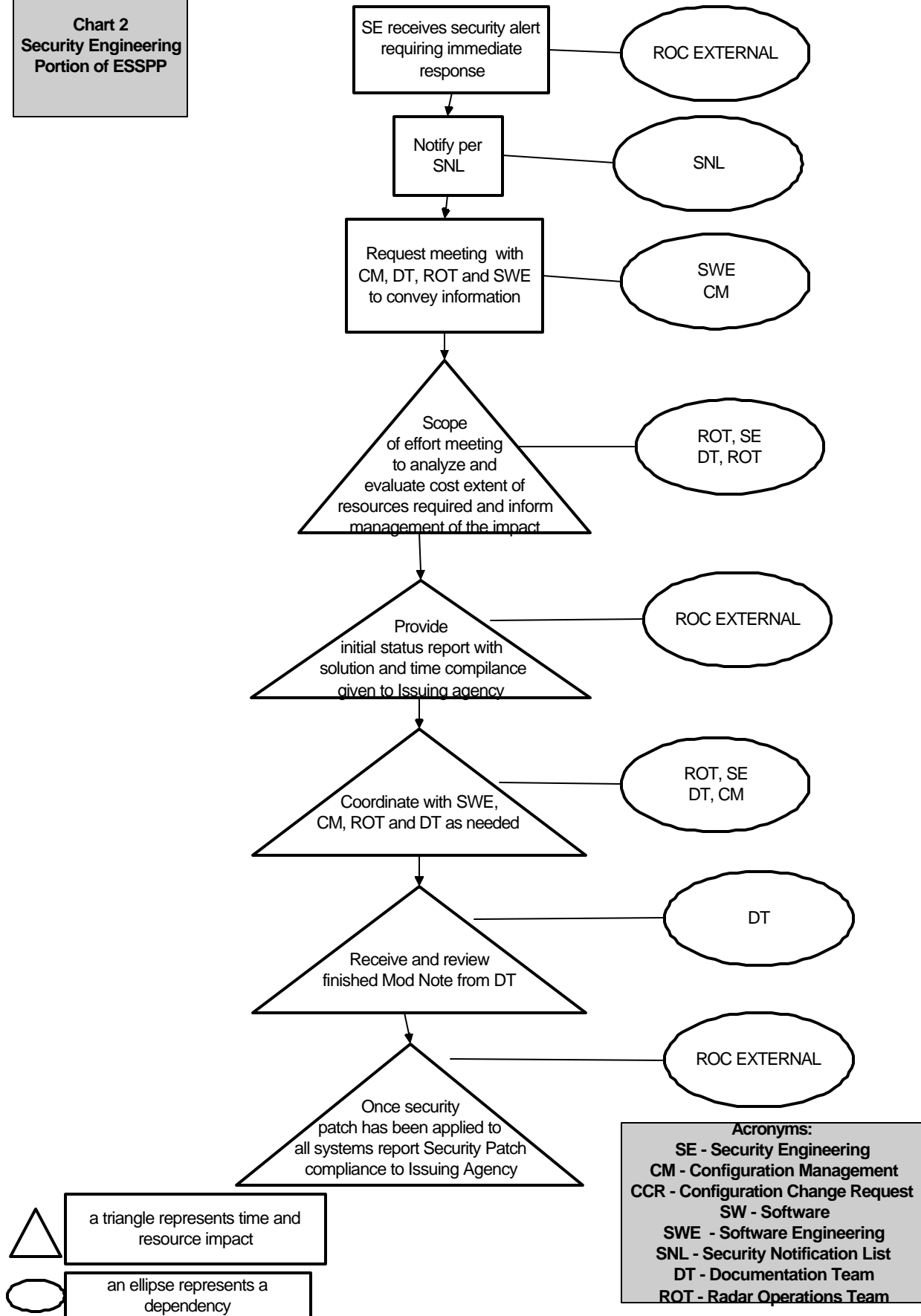
occur in specific ROC work sections. Some of the steps the ROC section oriented flowcharts are administrative in nature, yet crucial to the ultimate outcome of delivering a patch release to the radar sites. Triangles are used to indicate a time and resource impact, and an ellipse to indicate a dependency (either ROC internal or external).

**Chart 1  
Emergency System  
Security Patch  
Process**

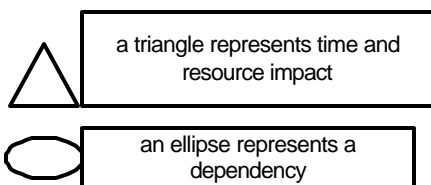
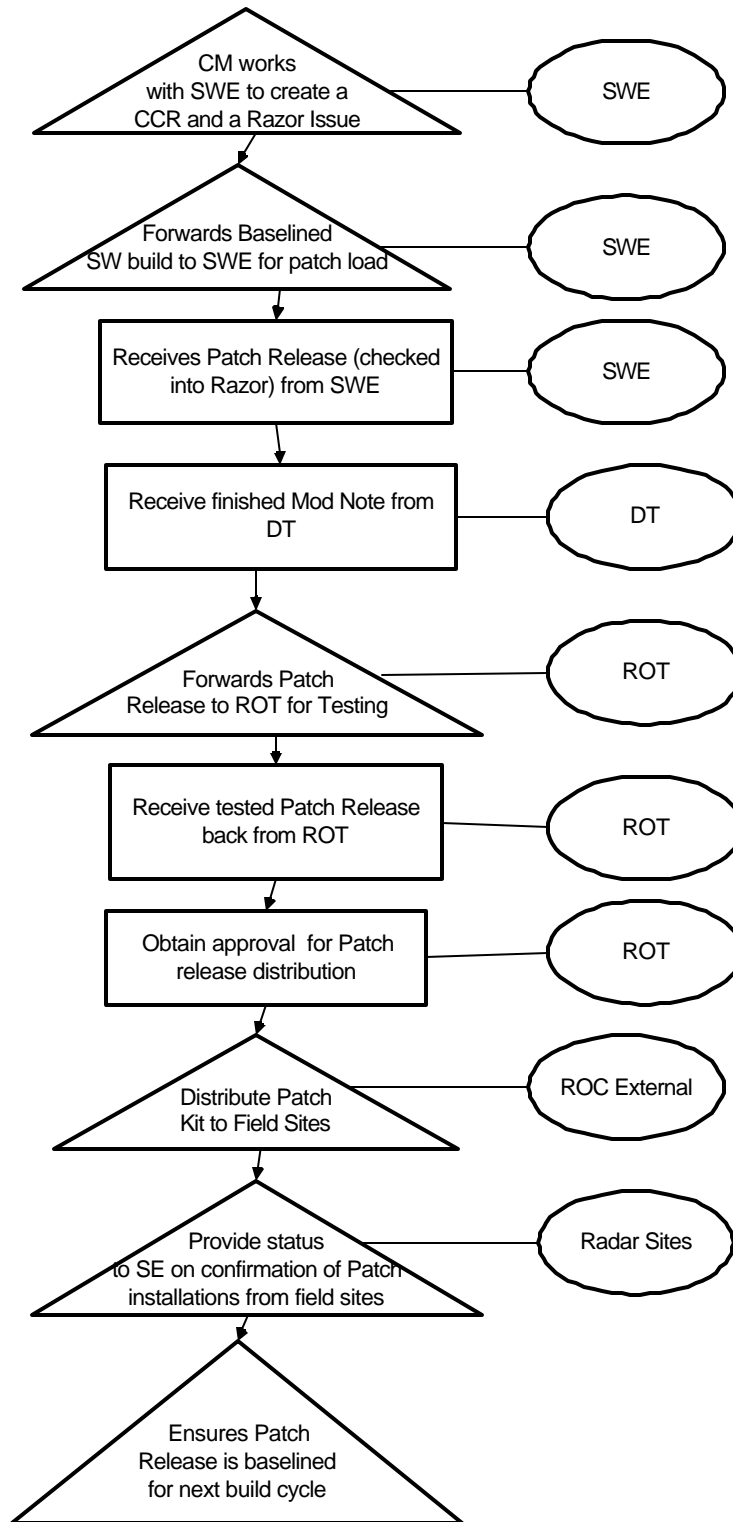


**Acronyms:**  
 SE - Security Engineering  
 CM - Configuration Management  
 CCR - Configuration Change Request  
 SW - Software  
 SWE - Software Engineering  
 DT - Documentation Team  
 ROT - Radar Operations Team

**Chart 2**  
**Security Engineering**  
**Portion of ESSPP**

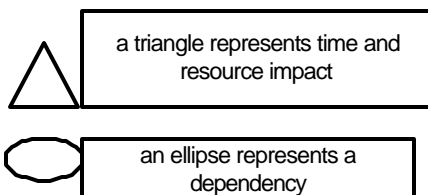
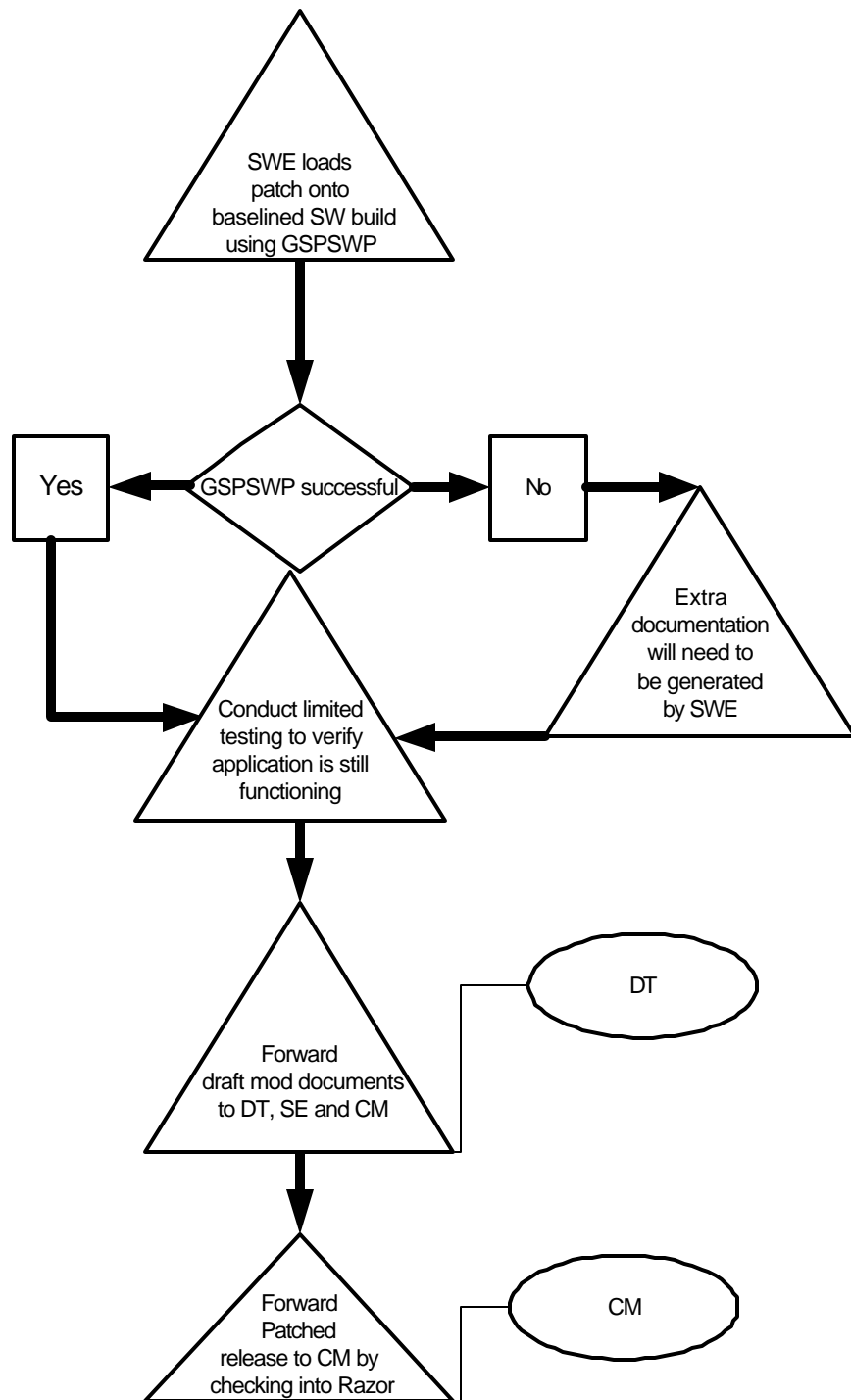


**Chart 3**  
Configuration  
Management portion  
of ESSPP



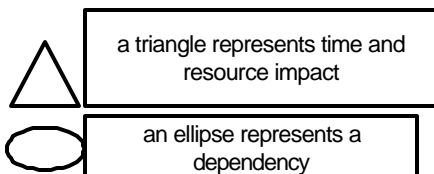
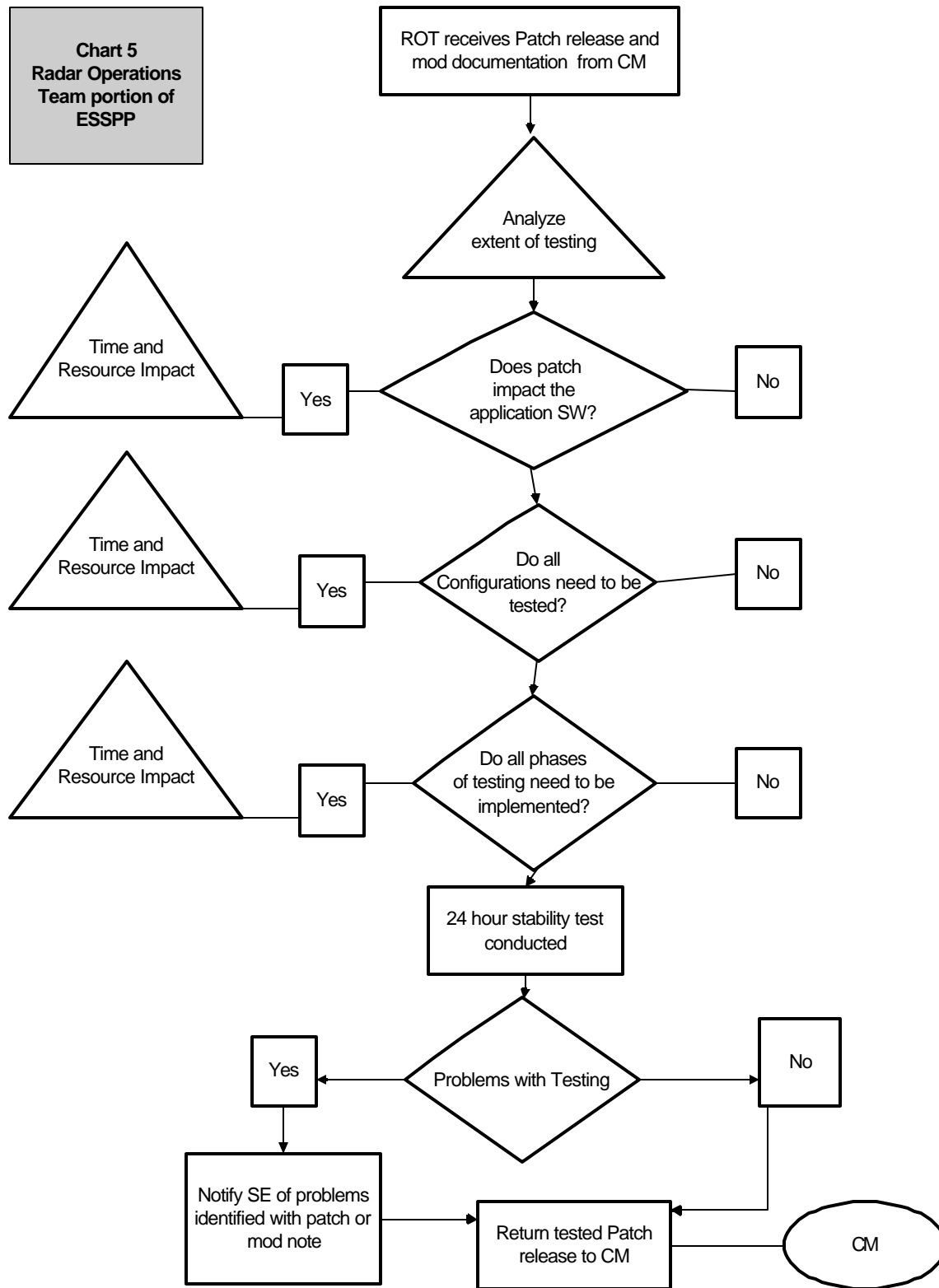
**Acronyms:**  
SE - Security Engineering  
CM - Configuration Management  
CCR - Configuration Change Request  
SW - Software  
SWE - Software Engineering  
DT - Documentation Team  
ROT - Radar Operations Team

**Chart 4**  
**Software**  
**Engineering portion**  
**of ESSPP**



**Acronyms:**  
 SE - Security Engineering  
 CM - Configuration Management  
 CCR - Configuration Change Request  
 SW - Software  
 SWE - Software Engineering  
 DT - Documentation Team  
 ROT - Radar Operations Team

**Chart 5**  
Radar Operations  
Team portion of  
ESSPP



**Acronyms:**  
SE - Security Engineering  
CM - Configuration Management  
CCR - Configuration Change Request  
SW - Software  
SWE - Software Engineering  
DT - Documentation Team  
ROT - Radar Operations Team

**Chart 6**  
Documentation  
Team portion of  
ESSPP

